COMPARISON CHART

DCS – Second Amended Complaint Madison County, Alabama June 13, 2023	**OU – First Amended Complaint** Northern District of Alabama July 19, 2023
P. 4-5 ¶ 16: "Oakwood claimed . . . under the parties' Service Agreement of May 1, 2019."	P. 6 ¶ 18: "Oakwood contracted with DCS on May 1, 2019."
P. 5 ¶ 17: "It's important to note that the parties' Service Agreement does NOT include IT support directly associated with security breaches and ransomware." P. 5 ¶ 17, Footnote 2: "Schedule A Statement of Work to the Parties' Agreement outlines DCS's responsibilities and absent from this detailed list is any mention of the provision of support directly associated with security breaches and/or ransomware."	P. 6 ¶ 19: "The Agreement obligated Dynamic Campus to provide services to ensure the security of Oakwood's IT Systems." "Dynamic Campus agreed to . . . generally help the University fend off and/or lessen the risks of a cyber-attack." P. 9 ¶ 29: "The University relied upon Dynamic Campus's expertise . . . including Dynamic Campus's obligation to help prevent the risks of a ransomware attack, and/or prepare the University for an effective response to such an attack, and/or reduce the University's potential losses from such an attack."
P. 5 ¶ 17, Footnote 2: "Schedule A Statement of Work to the Parties' Agreement outlines DCS's responsibilities and absent from this detailed list is any mention of the provision of support directly associated with security breaches and/or ransomware."	P. 8 ¶ 27: "The Agreement adopted and incorporated a lengthy 'Statement of Work.' This Statement describes the services Dynamic Campus would provide to Oakwood during the term of the Agreement."
P. 5 ¶ 17: "In March of 2022, Oakwood University was the victim of a cyber-attack committed by an unknown criminal. The third-party, unknown criminal infiltrated the Oakwood network and was able to compromise an elevated account assigned to DCS's system administrator."	P. 9 ¶ 30: "In March 2022, a Threat Actor emailed an infected attachment to a person using an Oakwood email address." P. 9 ¶ 31: "In March 2022, the University detected unauthorized activity that impacted the availability and functionality of its computer systems."
P. 5 ¶ 18: "The threat actor (a/k/a the unknown third-party criminal) was initially blocked by Carbon Black, an antivirus/antimalware system . . . but was able to work around Carbon Black to gain	P. 9 ¶ 32: "More specifically, between March 7, 2022, and March 14, 2022, the Threat Actor accessed the University's internal systems, including personal and confidential information."

administrative access. With full administrative privileges, the criminal spent a few days looking for personal/private information and systems to encrypt. After sending the PII to an external site, the criminal planted malware on a variety of machines to invoke at a future time. As a final step, on March 13, 2022, the criminal encrypted most running VMware servers and then the VMware infrastructure itself."	P. 10 ¶ 34: "The Threat Actor managed to introduce ransomware (or malware) into Oakwood's Email Server, and then access and control Oakwood's most vital IT Systems."
P. 5 ¶ 19: "The DCS Shared Services team quickly traced the problem to the Dell storage device [VNX and ExtremIO]. Dell support was contacted and in the course of trying to fix what Dell believed was a broken machine, Dell damaged the ExtremIO beyond repair, thereby locking out DCS's ability to recover the most current database of their key software, Jenzabar. During this time, Shared Services' techs reinstalled the VMware environment and were able to view the files. It was at that time the techs saw indications of the presence of ransomware infecting the environment."	P. 11-12 ¶ 36: "Dynamic Campus claims that it had arranged for data backups in a safe location, on a Dell storage device (called an 'ExtremIO storage device'). DCS then blames Dell for damaging the storage device, thereby depriving Oakwood from receiving the backups supposedly kept on the device." P. 12 ¶ 38: "Dynamic Campus completely relied on keeping Oakwood's data backups on a Dell storage device which was part of the same 'ecosystem' as Oakwood's IT systems."
P. 7-8 ¶ 22: "DCS . . . provided Oakwood documentary evidence to demonstrate that DCS complied with industry standards in the provision of information technology services." P. 7 ¶ 24: "Oakwood claims DCS failed to 'refresh, restore, and backup services for optimal service,' and that the last working backup dated back to 2019. This is false."	P. 11 ¶ 35: "Dynamic Campus also failed to keep fresh backups in a secure location . . . If Dynamic Campus had maintained fresh backups of Oakwood's data in a safe location, in accordance with industry standards, Oakwood could have restored the backups on new servers, resumed normal operations in a short time and ended the cyber-event (and the University would not have had to pay the Threat Actor the steep ransom)."
P. 7 ¶ 24: "Backups are a core part of the IT business and while it is not a common practice to document same, backups were maintained regularly and kept on a storage device. The actual dates of backup are embedded in the filename and evidence regular backups. Also, the backups were regularly tested. On numerous occasions prior to the criminal attack, backups were used to restore files and systems, and to provide a refresh to test pre-production environments. In a nutshell, the backups worked."	P. 12 ¶ 37: "Dynamic Campus had a duty (contractually and professionally) to keep Oakwood's backups in a location that could not be corrupted by ransomware or malware. Specifically, as noted above, DCS had a duty to 'test the backups to ensure the systems can be restored properly from the backups and as required and in preparation for an unforeseen disaster.' DCS failed to do so."
P. 7 ¶ 25: "DCS was unable to access the backups following the Incident as DCS did not have access to the	P. 10-11 ¶ 35: "Dynamic Campus stored pass keys or passwords to vital programs/systems in plain

configuration keys. Oakwood's system was configured and installed prior to DCS's involvement as the IT Service Provider. Oakwood was solely responsible to record the keys and pass them onto DCS, in order to provide DCS the right to access the configuration keys." P. 8 ¶ 26: "DCS has learned that CSPIRE, the vendor that configured the VEEAM backup solution for Oakwood prior to DCS becoming the IT service provider, had also not recorded the configuration keys."	sight (i.e., in a location easily accessible to and readable by a hacker). These indispensable "keys" were not encrypted or otherwise protected from view by an intruder into the University's IT Systems." "If Dynamic Campus had stored the keys in another location or in a way that prevented a third party from seeing or accessing them (for example, storing them off-site or encrypting them), the hacker would not have been able to gain control over Oakwood's entire system."
P. 11 ¶ 35: "Oakwood's claims of . . . breach of contract against DCS are spurious attempts to deflect attention from Oakwood's own negligent conduct and the negative impact of the criminal cyber-attack." P. 7 ¶ 25: "Throughout April 2022, DCS worked diligently to restore the backup of files. DCS was unable to access the backups following the incident as DCS did not have access to the configuration keys." "Oakwood was solely responsible to record the keys and pass them onto DCS, in order to provide DCS the right to access the configuration keys. Oakwood failed in its contractual obligation to provide same, which caused DCS's inability to access the backups following the criminal Ransomware Incident." P. 10 ¶ 31: "There is nothing in the parties' Service Agreement that says DCS's services includes or warrants the prevention of cyber-attacks. DCS complied with community standards in providing IT services and in implementing commercially reasonable steps to combat the attack. And, as explained above, DCS provide regular backup for Oakwood's system and data." P. 9 ¶ 30: "In fact, DCS went well beyond the scope of work laid out in the Parties' Service Agreement, at no additional cost to Oakwood, to help Oakwood recover from the Ransomware Incident. This entailed DCS providing out of contract services and additional hours at no extra charge."	**COUNT I – BREACH OF CONTRACT** P. 15 ¶ 48: "Dynamic Campus breached the Agreement and caused, contributed to, or was a causal factor in the ransomware attack by leaving the keys to Oakwood's IT systems in an area easily accessible to hackers and failing to ensure fresh backups were available to Oakwood." P. 15 ¶ 49: "As a result of Dynamic Campus's breach of the parties' Agreement, Oakwood suffered extensive damages, including being forced to pay a ransom to the Threat Actor and having to pay a massive cybersecurity premium increase due to, among other items, insurance claims made because of the Attack itself and Dynamic Campus's unsatisfactory management of Oakwood's cyber controls." P. 15 ¶ 50: "Oakwood also . . . experienced significant additional labor costs due to Oakwood staff working long and unexpected hours to compensate for restoration delays caused by Dynamic Campus."

P. 8 ¶ 26: "DCS cannot be blamed for any alleged loss, damage, or destruction or inability of Oakwood to use any service, system or program as there was nothing DCS did or failed to do that amounted to negligent conduct." P. 8 ¶ 27: "This unique situation . . . was caused by an unknown criminal encrypting the backup system AND neither the system's vendor, CSPIRE, nor Oakwood had the original configuration information which was necessary under this unique situation. DCS shares no blame or negligence for actions or failures to act under circumstances under which it had no control." P. 9 ¶ 30: "DCS's inability to access the configuration keys was due to no negligence on DCS's part, and, in fact, was due to Oakwood's failure to comply with its contractual obligation." P. 11 ¶ 35: "Oakwood's claims of professional negligence and/or breach of contract against DCS are spurious attempts to deflect attention from Oakwood's own negligent conduct and the negative impact of the criminal cyber-attack."	**COUNT II – NEGLIGENCE** **COUNT III – WANTONNESS** P. 16 ¶ 54: "Dynamic Campus owed Oakwood duties concerning its IT Systems. These duties included exercising reasonable care in ensuring the security of Oakwood's IT Systems and preparing the University to effectively and promptly respond to a cybersecurity event to eliminate or minimize the potential risks." P. 16 ¶ 55: "Dynamic Campus breached that duty by failing to act as a reasonable IT Systems professional and/or Shared Services Provider in various ways." P. 17 ¶ 56: "Dynamic Campus knew and could foresee that a Threat Actor could identify, read, and access the keys/password after gaining access to Oakwood's Email Server, yet it utterly failed to protect such data from the foreseeable damage that a Threat Actor could wreak with access to that information." P. 17 ¶ 58: "Dynamic Campus knew and could foresee that failure to maintain fresh, safe and easily accessible data increased the risk of danger and damage from a Threat Actor's attack."
P. 7-8 ¶ 22: "DCS . . . provided Oakwood documentary evidence to demonstrate that DCS complied with industry standards in the provision of information technology services." P. 7 ¶ 24: "Oakwood claims DCS failed to 'refresh, restore, and backup services for optimal service,' and that the last working backup dated back to 2019. This is false." "Backups are a core part of the IT business and while it is not a common practice to document same, backups were maintained regularly and kept on a storage device. The actual dates of backup are embedded in the filename and evidence regular backups. Also, the backups were regularly tested. On numerous occasions prior to the criminal attack, backups were used	**COUNT VI – PROMISSORY FRAUD** **COUNT V – FRAUDULENT SUPPRESSION** **COUNT VI – NEGLIGENT MISREPRESENTATION** P. 19 ¶ 71: "Dynamic Campus's false promises and misrepresentations induced Oakwood to act or refrain from acting, including, without limitation: (a) ensuring Oakwood had another, alternative backup service in case of a cybersecurity attack by a Threat Actor; and (b) refraining from requesting Dynamic Campus to ensure proper storage of necessary credentials and passwords related to Oakwood's backup servers." P. 20 ¶ 77: "Dynamic Campus suppressed material information regarding its acts and omissions

to restore files and systems, and to provide a refresh to test pre-production environments. In a nutshell, the backups worked." P. 7 ¶ 25: "DCS was unable to access the backups following the Incident as DCS did not have access to the configuration keys. Oakwood's system was configured and installed prior to DCS's involvement as the IT Service Provider. Oakwood was solely responsible to record the keys and pass them onto DCS, in order to provide DCS the right to access the configuration keys." P. 8 ¶ 26: "DCS has learned that CSPIRE, the vendor that configured the VEEAM backup solution for Oakwood prior to DCS becoming the IT service provider, had also not recorded the configuration keys." P. 8 ¶ 27: "This unique situation . . . was caused by an unknown criminal encrypting the backup system AND neither the system's vendor, CSPIRE, nor Oakwood had the original configuration information which was necessary under this unique situation. DCS shares no blame or negligence for actions or failures to act under circumstances under which it had no control." P. 9 ¶ 30: "DCS's inability to access the configuration keys was due to no negligence on DCS's part, and, in fact, was due to Oakwood's failure to comply with its contractual obligation." P. 11 ¶ 35: "Oakwood's claims of professional negligence and/or breach of contract against DCS are spurious attempts to deflect attention from Oakwood's own negligent conduct and the negative impact of the criminal cyber-attack."	concerning data security and the fact that it was not making timely backups of Oakwood's servers and other data server backups before, during, and after the Attack."